Security Procedure

Policy: See N-03 Passwords at www.cosdcompliance.org

Definitions: See HHSA Policy N-13 Security Definitions

Procedures:

A. Create Strong Passwords:

1. Passwords must be created according to the County network password requirements:
   - Password must have a minimum of eight (8) characters in length, may not contain user account name or user's full name, or any other personal identifiable information.
     - For telephones and smartphones, the passcode or PIN # must not contain easily guessed numbers such as the device phone number or 1234.
   - Password must contain at least one character from three of the following four groups:
     - Uppercase letters (A through Z)
     - Lowercase letters (a through z)
     - Numbers (0 through 9)
     - Keyboard special characters (e.g. !@$%^&*)

2. Create a strong password that can easily be remembered to avoid writing it down (e.g. 4U2Know!).

B. Protect Passwords:

Each account owner is responsible for ALL activity performed by his/her username and password. Therefore,

1. A password is confidential information and is not to be shared with anyone (e.g. Manager/supervisor, co-worker, IT technical staff) under any circumstance. The account owner must take all reasonable care to protect his/her password from being used by someone else. This includes the following situations when the user is:
   - Transferring out
   - Retiring or terminating employment with the County
   - Going on vacation
   - Going on extended leave

   Please contact the Agency Compliance Office at 619-338-2634 for assistance if access to the user's emails or files need to be retrieved after the user has left. A business justification will be required.

2. The same password for other systems should not be used.

3. An incorrect password consecutively entered five or less times must lock or suspend the account. The account owner is to contact the appropriate system administrator to unlock or request a password reset.

C. <u>Change Password Frequently:</u>

1. Password must be changed at least every 90 days.

2. A password must not be re-used. Password history: 24 passwords.

3. A password must be changed immediately if it has been revealed or is suspected to have been compromised. Change your password at once if you notice any unusual activity occurring with your account (e.g. files are missing or have been modified).

   - To change your password, on the keyboard press ‘**Ctrl, Alt, and Delete’** at the same time. A pop- up menu will appear. Click on “Change Password” and change your password.

4. After the initial or default password has been entered, the system must prompt the user to change the password to their own.

5. For password resets:

   - County employees are to contact the appropriate system administrator (e.g. County Help Desk, application administrator) to request a password reset. The employee’s identity must be verified prior to resetting the password.

   - Non-County employees are to contact their County sponsor to request a password reset. The County sponsor verifies the identity of the non-County user before calling the appropriate Password Reset Authorizer or System Administrator to request a password reset on behalf of the non-County user.

D. <u>Password Reset Authorizers</u>

Only appointed password reset authorizers and system administrators are authorized to reset passwords at the request of the account owner or the non-County employee’s County sponsor. The user’s identity must be verified each time prior to resetting the password.

Violations or suspected violations of this policy will be referred to the Agency Human Resources for appropriate personnel action or investigation.

<u>QUESTIONS/INFORMATION</u>: HHSA Information Security Manager at 619-338-2634